

# INFORMATION SYSTEMS SECURITY PROGRAM MANAGEMENT

FISMA / NIST

REFERENCE SECTION

VERSION 1

LAST UPDATE 2/22/10

## MODULE 1

INTRODUCTION TO INFORMATION SECURITY MANAGEMENT

INTRODUCTION TO INFORMATION SYSTEMS SECURITY MANAGEMENT

### REVIEW

[Presentation: Information Security Governance.pdf](#)

[NIST SP 800-100: Chapter 2 Information Security Governance.pdf](#)

[NIST SP 800-100: Information Security Governance Frequently Asked Questions.pdf](#)

[NIST Glossary Of Key Information Security Terms.pdf](#)

[NIST SP 800-100: Acronyms List.pdf](#)

[Information Security Terminology.pdf](#)

[Data Lifecycle Security.pdf](#)

[Information Technology / Information Security Essential Body Of Knowledge.pdf](#)

[Information Security Regulations And Compliance Management-Video Based.url](#)

### REFERENCE

[NIST SP 800-100: Information Security Handbook-Guide For Managers.pdf](#)

[NIST SP 800-14: Generally Accepted Principles For Securing IT Systems.pdf](#)

[CERT-Governing for Enterprise Security Implementation Guide.pdf](#)

[Effective Versus In-Effective Security Governance.pdf](#)

### FEDERAL AGENCIES SECURITY HANDBOOKS

[Health And Human Services Information Security Program Handbook.pdf](#)

[Dept. Of Commerce IT Security Program Policy And Minimum Implementation Standards.pdf](#)

[Dept. Of Veterans Affairs Information Security Handbook.pdf](#)

[USDA Information Security Program Manual.pdf](#)

[CMS Policy For The Information Security Program.pdf](#)

[Dept. Of Energy IT Security Architecture.pdf](#)

### IA POLICY CHARTS

[DOD IA Policy Chart / Trusted GIG IA Policy Chart.url](#)

## MODULE 2A

FISMA / FEDERAL INFORMATION SECURITY MANAGEMENT ACT

### REVIEW

[Presentation: FISMA Overview.pdf](#)

[Presentation: FISMA Implementation Project.pdf](#)

[FISMA Security Controls Overview.pdf](#)

[FISMA Steps.pdf](#)

### OMB/NIST Guidance On New FISMA Metrics

[OMB/NIST Release Draft Of New FISMA Metrics.url](#)

[OMB-FY2010 Security Metrics.pdf](#)

[FISMA Reporting For 2010.url](#)

### REFERENCE

#### FISMA

[FISMA Implementation Project.url](#)

[Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources.pdf](#)

[E-Government Act Of 2002.pdf](#)

[FISMA Compliance Vs Security.pdf](#)

[FISMA Preparing For A FISMA Audit.pdf](#)

#### **FISMA REPORTING**

[FISMA FY 2008 Reporting Instructions For FISMA And Agency Privacy Management.pdf](#)

[FY 2008 FISMA Reporting FAQ.pdf](#)

#### **FISMA AUDIT REPORTS EXAMPLES**

[FISMA Audit Report For Dept. Of Homeland Security.pdf](#)

[FISMA Audit Report For GSA IT Security Program.pdf](#)

#### **FISMA MANAGEMENT TOOLS**

[EPA ASSERT FISMA Reporting Software.url](#) (Free)

[OpenFISMA.url](#)

[OpenFISMA Overview.pdf](#)

## **MODULE 2B**

### **NATIONAL SECURITY SYSTEMS**

#### **DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY AGENCIES**

#### **REVIEW**

[NIST SP 800-59: Guideline For Identifying An Information System As A National Security System.pdf](#)

[Committee On National Security Systems/CNSS: Information Assurance Glossary.pdf](#)

#### **REFERENCE**

[Department Of Defense And Intelligence Community Agencies Regulations.url](#)

## **MODULE 3**

### **NIST SPECIAL PUBLICATIONS**

#### **REVIEW**

[Presentation: NIST Special Publications.pdf](#)

[NIST Special Publications.url](#)

[NIST Special Publications Mailing List.url](#)

[NIST FIPS Publications.url](#)

[NIST Draft Publications.url](#)

[FIPS-NIST Publications Overview.pdf](#)

## **MODULE 4**

### **SECURITY CATEGORIZATION**

#### **FEDERAL INFORMATION / FEDERAL INFORMATION SYSTEMS**

#### **REVIEW**

[Presentation: Security Categorization Of Information Systems.pdf](#)

[FIPS-PUB-199: Standards for Security Categorization of Federal Information and Information Systems.pdf](#)

[NIST FAQ: For Security Categorization Standards For Information And Information Systems.url](#)

[CNSS 1253: Security Categorization And Control Selection For National Security Systems.pdf](#)

#### **REFERENCE**

[NIST SP 800-60 Volume 1: Guide For Mapping Types Of Information-Systems To Security Categories.pdf](#)

[NIST SP 800-60 Volume 2 : Appendices To Volume 1.pdf](#)

## **MODULE 5**

### **BASELINE SECURITY CONTROLS**

#### **FEDERAL INFORMATION / FEDERAL INFORMATION SYSTEMS**

#### **REVIEW**

#### **SECURITY CONTROLS**

[Presentation: Baseline Security Controls.pdf](#)

[FISMA Security Controls Overview.pdf](#)  
[FIPS-200: Minimum Security Requirements for Federal Information and Information Systems.pdf](#)  
[NIST SP 800-53R3: Recommended Security Controls For Federal Information Systems.pdf](#)  
[NIST SP 800-53R3: Appendix G: Information Security Program Controls.pdf](#)  
[NIST SP 800-53R3: Appendix D: Security Controls Summary Listing For L-M-H Baselines.pdf](#)  
[NIST SP 800-53R3: Appendix F: Security Control Catalog.pdf](#)  
[NIST SP 800-53: NIST To DCID 6/3 Security Controls Mappings.pdf](#)  
[NIST SP 800-53: CMS Management, Operational, And Technical Security Controls Overview.pdf](#)  
[Baseline Security Controls For Classified Information Systems.pdf](#)  
[OMB-Memo 06-16: Protection Sensitive Information-Removed From/Accessed From Outside Agency.pdf](#)

## **REFERENCE**

### **SECURITY CONTROLS DATABASE**

[NIST SP 800-53: Security Controls Database Application Overview.pdf](#)  
[NIST SP 800-53: Security Controls Database Application.url](#)  
[NIST SP 800-53: Security Controls Database Quick Reference Guide.pdf](#)

### **SECURITY CONTROLS ASSESSMENTS AND CHECKLISTS**

[NIST SP 800-53A: Presentation On Assessment Procedures-1.pdf](#)  
[NIST SP 800-53A: Presentation On Assessment Procedures-2.pdf](#)  
[NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems.pdf](#)  
[NIST SP 800-53A: Security Control Assessment Process Chart.pdf](#)  
[NIST SP 800-53A: Appendix D-- Assessment Method Descriptions.pdf](#)  
[NIST SP 800-53A: Appendix E-- Assessment Expectations.pdf](#)  
[NIST SP 800-53A: Appendix F-- Security Control Assessment Procedures.pdf](#)  
[NIST SP 800-53A: Expanded Security Control Assessment Procedures.url](#)  
[NIST SP 800-53A: Appendix I-- Security Assessment Reports.pdf](#)  
[NIST SP 800-53: Security Controls Assessment Form.pdf](#)  
[NIST SP 800-53: Minimum Technical Security Configurations For Operating Systems, Oracle Database And Cisco Routers.pdf](#)  
[NIST SP 800-68: Guide To Securing Windows XP Pro Appendix C-Mapping XP Controls To NIST SP 800-53.pdf](#)  
[Information Security Program Audit Checklist Based On FIPS200-NIST SP 800-53.pdf](#)

### **CONSENSUS AUDIT GUIDELINES** (20 Specific Security Controls That Are Essential For Blocking Known High-Priority Attacks)

[Consensus Audit Guidelines No Substitute For FISMA Guidance.url](#)  
[Consensus Audit Guidelines Overview.url](#)  
[Consensus Audit Guidelines / Description Of Controls.url](#)

### **COMMITTEE ON NATIONAL SECURITY SYSTEMS/CNSS**

[CNSS 1253: Security Categorization And Control Selection For National Security Systems.pdf](#)  
[Overview of NIST SP 800-53 Rev. 3 and CNSSI 1253.ppt](#)  
[CNSS Instruction 1253 Security Control Mapping Table.pdf](#)  
[CNSS Instruction 1253 MappingTo DOD 8500.2.xls](#)

## **MODULE 6**

### **SECURE CONFIGURATION OF INFORMATION SYSTEMS**

#### **HARDWARE / OPERATING SYSTEMS / SOFTWARE APPLICATIONS**

## **REVIEW**

[Presentation: Secure Configuration Information Systems.pdf](#)  
[NIST SP 800-123 Guide To General Server Security Overview.pdf](#)  
[NIST SP 800-44 Guide On Securing Public Web Servers Overview.pdf](#)  
[NIST SP 800-95 Guide Secure Web Services Overview.pdf](#)  
[Federal Desktop Core Configuration Training.url](#)  
[Federal Desktop Core Configuration/FDCC FAQ.pdf](#)  
[Best Practices For Hardening Host Systems-Video Based.url](#)

## **REFERENCE**

### **ADMINISTRATOR ACCOUNT SECURITY**

[Microsoft Administrator Accounts Security Planning Guide.pdf](#)

### **DESKTOP AND SERVER SECURITY**

[OMB Memo 07-11: Implementation Of Security Configurations For Microsoft Windows.pdf](#)

### **SECURE CONFIGURATION CHECKLISTS FOR OPERATING SYSTEMS AND APPLICATIONS**

[NIST SP 800-123: Guide To General Server Security.pdf](#)

[NIST SP 800-70: Overview Checklists Program For IT Products.pdf](#)  
[Federal Desktop Core Configuration Home Page.url](#)  
[Federal Desktop Core Configuration Download Page.url](#)  
[Overview Of NIST SCAP FDCC Scanners For Secure Configuration Verification.url](#)  
[National Checklist Program Repository.url](#)  
[NIST Security Configuration Checklists.url](#)  
[NIST SCAP Security Checklists.url](#)  
[NIST SP 800-53: Minimum Technical Security Configurations For Operating Systems, Oracle Database And Cisco Routers.pdf](#)  
[Center For Internet Security Standards.url](#)  
[DSS DAA Tools.url](#)

[DSS Baseline Security Configurations For Windows 2000/XP-Windows Server 2003.pdf](#)  
[DISA Security Technical Implementation Guides/STIGS.url](#)  
[DISA Security Checklists.url](#)  
[NSA Security Configuration Guides.url](#) (Click IA Guidance Link On Left)  
**MICROSOFT WINDOWS XP / WINDOWS VISTA / WINDOWS 2003 SERVER / WINDOWS 2008 SERVER**  
[Microsoft Security and Compliance Guides.url](#)  
[Microsoft Security Compliance Management Toolkit.url](#) (Windows XP, Windows Vista, Windows Server 2003)  
[Microsoft Threats And Countermeasures Security Settings For Windows Server 2003/XP.url](#)  
[Microsoft Windows XP Security Guide.url](#)  
[Microsoft Windows Vista Security Guide.url](#)  
[Microsoft Windows Server 2003 Security Guide.url](#)  
[Microsoft Windows Server 2008 Security Guide.url](#)  
[Microsoft Windows Server 2008 Server Core Overview.url](#)  
[Microsoft Windows Server 2008 Server Core Secure Configuration Option.url](#)  
[Microsoft Windows Services and Service Accounts Security Planning Guide.url](#)  
[Microsoft Windows Services.url](#) (Explanations On Which Services Can Be Safely Disabled)  
[NIST SP 800-68: Guide To Securing Microsoft Windows XP Systems.pdf](#)  
[NIST Windows Security Baseline Database.url](#) (Under Download Packages)  
[Microsoft Windows SteadyState.url](#)  
[Microsoft Windows Steady State: Protecting Public-Shared Access Computers Part 1.pdf](#)  
[Microsoft Windows Steady State: Protecting Public-Shared Access Computers Part 2.pdf](#)  
[Faronics Deep Freeze.url](#)

**MICROSOFT WINDOWS GROUP POLICY SECURITY**  
[Microsoft Windows Group Policy Security.url](#)  
[Microsoft Windows Group Policy Inventory Tool.url](#)  
[Microsoft GPO Accelerator Tool Creates Group Policy Objects For Recommended Security Settings.url](#)

**MICROSOFT WINDOWS ACTIVE DIRECTORY SECURITY**  
[Microsoft: Best Practice Guide for Securing Active Directory Installations.url](#)  
[Microsoft: Securing Active Directory.url](#)  
[Microsoft: Securing Active Directory Administrative Groups and Accounts.url](#)  
[Microsoft: 19 Smart Tips for Securing Active Directory.url](#)  
[Securing Windows 2000 Active Directory Part 1.url](#)  
[Securing Windows 2000 Active Directory Part 2.url](#)

**MICROSOFT OFFICE SECURITY**  
[Microsoft Office 2007 Security Guide.url](#)

**MICROSOFT ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES**  
[Define Who Can Open, Modify, Print, Forward, Or Take Other Actions With Digital Information](#)  
[Active Directory Rights Management Services.url](#)  
[Active Directory Rights Management Services Demo's.url](#)  
[Licensing Windows Rights Management Services.url](#)

**DOMAIN NAME SYSTEM / DNS SECURITY**  
[OMB Memo-M-08-23 Securing Federal Government DNS Infrastructure.pdf](#)  
[NIST SP 800-81: Secure Domain Name System Deployment Guide.pdf](#)

**WEBSITES / WEB APPLICATION SECURITY / INTERNET SECURITY**  
[OMB Policies For Federal Public Websites.url](#)  
[SANS Top 25 Most Dangerous Programming Errors.url](#)  
[NIST SP 800-44 Guidelines On Securing Public Servers.pdf](#)  
[NIST SP 800-95: Guide To Secure Web Services.pdf](#)  
[NIST SP 800-28: Guidelines On Active Content And Mobile Code.pdf](#)

[HP Offers Free Security Tool For Flash Developers.url](#)

[HP SWFScan Download.url](#)

[Open Web Application Security Project.url](#)

[DHS Software Assurance Resources.url](#)

#### **MACINTOSH SECURITY**

[NSA Hardening Tips For Mac Operating System.pdf](#)

[SecureMac Apple Macintosh Security.url](#)

#### **UNIX / LINUX SECURITY**

[NSA Security-Enhanced Linux.url](#)

[Trusted Computer Solutions: Security Blanket-Automates Lockdown / Hardening Of Linux Servers.url](#) (DISA / DCID / JAFAN)

[Linux Gets Common Criteria Certification.url](#)

[LinuxSecurity.Com](#)

[Linux Security Quick Reference Guide.pdf](#)

[Unix Security Overview.pdf](#)

#### **TRUSTED MODULE PLATFORM / TPM CHIP**

[Trusted Platform Module Chip.pdf](#)

[Trusted Computing Group.url](#)

[Managing TPM Chip.url](#)

[Microsoft TPM Management Console/MMC Snap-In.url](#)

[Wave Trusted Computing TPM Management Software.url](#)

#### **VMWARE AND MICROSOFT VIRTUAL SERVER SECURITY**

[VMWARE: Understanding Security in a Virtualized Environment.url](#)

[Securing VMware Report.pdf](#)

[Windows Server 2008 Hyper-V.url](#)

[Microsoft Virtual PC 2007.url](#)

[Virtualization And Security Video.url](#)

[Third Brigade VM Protection.url](#) (Free--Firewall, IDS, Integrity Monitoring And Log Inspection)

#### **USB PORT SECURITY**

[USBDeview - View Installed-Previously Connected USB Devices On System.url](#)

[Advanced Force USB LockDown.url](#)

[DeviceLock.url](#)

[DeviceWall.url](#)

[AccessPatrol.url](#)

[GFI EndPoint Security.url](#)

[Safend Auditor / Safend Protector.url](#)

[USB Write Block.url](#)

[NSA Brochure-Disabling USB Ports.pdf](#)

[Video Disable USB Storage Under OS X or Windows.url](#)

[How To Disable USB And CD-ROM On A Windows Network Using Group Policy.url](#)

[How To Use Device Installation Restrictions To Control USB Devices On Windows Vista.url](#)

[Have Your Lost USB Drive Ask For Help.url](#)

#### **FIREWALLS**

[NIST SP 800-41: Guidelines On Firewalls And Firewall Policy.pdf](#)

[TCP/IP Port Numbers \(TCP-UDP\).url](#)

[Microsoft Windows XP Commonly Used TCP/IP Ports.pdf](#)

[DOD Ports, Protocols And Services Management.url](#)

#### **ROUTER / SWITCH SECURITY**

[Cisco Learning Center.url](#)

[Cisco IOS And NX-OS Software: Using The Command-Line Interface In Cisco IOS Software.url](#)

[Cisco IOS Network Management Command Reference.url](#)

[Cisco IOS Security.url](#)

[Cisco Guide to Hardening Cisco IOS Devices.pdf](#)

[CiscoWorks Network Compliance Manager.url](#)

[Securing Cisco Switches Training.url](#)

[NSA Cisco Router Security Configuration Guides.url](#)

[How To Properly Secure A Cisco Router With Passwords.url](#)

[Nipper Router, Switch And Firewall Auditing Tool.url](#)

#### **WIRELESS SECURITY**

[Wireless AutoSwitch.url](#) (Auto-Disable Wireless Card When Connected To LAN / Auto-Enable When There Is No LAN Connection)

#### **ANTI-VIRUS AND MALICIOUS CODE SECURITY**

[NIST SP 800-83: Guide To Malware Incident Prevention and Handling.pdf](#)

[Microsoft Antivirus Defense-In-Depth Guide.pdf](#)

[Symantec Report: Impact Of Malicious Code On Windows Vista.pdf](#)

#### **DISK ENCRYPTION SOFTWARE**

[Windows Encrypting File System-Controlling Using Group Policy.pdf](#)

[Windows Vista BitLocker Drive Encryption.url](#)

[Windows Vista BitLocker Drive Encryption Configuration Guide.url](#)

[Disk Encryption Applications Put A Lock On Data.pdf](#)

[Data Locker Portable USB Hard Drive With Encryption.pdf](#)

[Hard Drives With Built In Encryption.url](#)

[Encrypt Them All.pdf](#)

#### **E-MAIL SECURITY**

[NIST SP 800-45 Guidelines On Electronic Mail Security.pdf](#)

#### **INFORMATION ARCHITECTURE SECURITY**

[Dept. Of Energy IT Security Architecture.pdf](#)

## **MODULE 7**

### **INTER-CONNECTING INFORMATION SYSTEMS**

#### **REVIEW**

[Presentation: Inter-Connecting Information Systems.pdf](#)

[NIST SP 800-100: Chapter 6 Overview Inter-Connecting Systems.pdf](#)

#### **REFERENCE**

[NIST SP 800-47: Security Guide For Inter-Connecting IT Systems.pdf](#)

[NIST SP 800-47: Inter-Connection Security Agreement.pdf](#)

[NIST SP 800-47: Sample Memo of Understanding.pdf](#)

## **MODULE 8**

### **PRIVACY**

#### **PERSONALLY IDENTIFIABLE INFORMATION / PII PROTECTION**

#### **PRIVACY IMPACT ASSESSMENTS / PIA**

#### **REVIEW**

##### **PRIVACY OVERVIEW**

[OMB Privacy Memo Summaries.pdf](#)

[Presentation: Privacy Rules of Conduct.pdf](#)

[DOD Privacy Rules Of Behavior-Acceptable Use Policy.pdf](#)

##### **PRIVACY TRAINING**

[Presentation: Privacy Act Training 2006.pdf](#)

[Presentation: Protecting PII.pdf](#)

[National Institutes of Health Privacy Awareness Training.url](#)

[DOD Training: Personally Identifiable Information/PII.url](#)

[DHS Privacy Handbook-Safeguarding PII.pdf](#)

[NAVY Privacy Training.url](#)

[Federal Trade Commission: Brochure- Protecting Personal Information--A Guide For Business.pdf](#)

[Federal Trade Commission: Video- Protecting Personal Information--A Guide for Business.url](#)

#### **REFERENCE**

[Dept. Of Justice: Overview Of The Privacy Act of 1974.url](#)

[NIST SP 800-122: Guide to Protecting the Confidentiality Of PII.pdf](#)

[GSA Guide: Protecting Personally Identifiable Information.pdf](#)

[Privacy Controls Framework.pdf](#)

[Privacy Requirements Reference And Checklist.pdf](#)

[Safeguarding PII In The Federal Government.pdf](#)

[Privacy And The Federal Government.pdf](#)

[Using Social Security Numbers As Forms Of Identification.pdf](#)

##### **PRIVACY IMPACT ASSESSMENTS**

[Privacy Impact Assessments Overview.pdf](#)

[Privacy Impact Assessment Training.url](#)

[Privacy Impact Assessment Guidance From OMB.url \(Conducting Privacy Impact Assessments / Privacy Policies on Websites\)](#)

[Privacy Impact Assessments On Systems Containing Federal Employees-Contractors PII.pdf](#)

[Health And Human Services Presentation/HHS: Privacy Impact Assessments.ppt](#)

[HHS Privacy Impact Assessment Guide.doc](#)

[HHS Privacy Impact Assessment Analysis Worksheet.doc](#)

[USDA Privacy Impact Assessment Template.pdf](#)

#### **OFFICE MANAGEMENT BUDGET / PRIVACY MEMOS AND PRIVACY GUIDANCE**

[OMB Privacy Guidance Website.url](#)

[OMB Memo 07-16: Safeguarding Against-Responding To Breach Of PII.pdf](#)

[OMB Memo 07-16: Sensitive Database Extracts Technical Frequently Asked Questions.pdf](#)

[OMB Memo 06-19: Reporting Incidents Involving PII-Incorporate Cost Into IT Investments.pdf](#)

[OMB-Memo 06-16: Protection Sensitive Information-Removed From/Accessed From Outside Agency.pdf](#)

[OMB Memo 06-16: Checklist Privacy Controls Assessment Template.xls](#)

[OMB Memo 06-15: Safeguarding Personally Identifiable Information.pdf](#)

[OMB Memo 05-08: Designation of Senior Agency Officials for Privacy.pdf](#)

[OMB Memo 03-22: Guidance Implementing Privacy Impact Assessments \(When/How\) Per The E-Government Act 2002.url](#)

[OMB Memo 00-13: Privacy Policies And Data Collection On Federal Web Sites.url](#)

[OMB Memo: Recommendations for Identity Theft Related Data Breach Notification.pdf](#)

#### **PRIVACY AND DATA BREACHES**

[PII Breach Response Team Charter.pdf](#)

[Policy For Responding To Breaches Of PII.pdf](#)

[CMS InfoSec Incident Handling And Breach Analysis-Notification Procedure.pdf](#)

[Privacy Breach-Privacy Breach Notifications.pdf](#)

[Data Breach Notification Laws By State As of 10.19.07.pdf](#)

[Data Breach Notification Laws, State By State.url](#)

[Privacy-Data Protection Checklist.pdf](#)

#### **WEBSITE PRIVACY POLICIES**

[COPPA-Childrens Online Privacy Protection Act For Websites.pdf](#)

[Webcontent.gov - Guide to Managing U.S. Government Websites Privacy Policies and Cookies.url](#)

[Webcontent.gov - Guide to Managing U.S. Government Websites.url](#)

#### **SOFTWARE TOOL TO SCAN FILES FOR PERSONALLY IDENTIFIABLE INFORMATION/PII**

[Scan For Social Security Numbers Or Credit Card Numbers.url](#) (Free Tool)

[Identity Finder Theft and Data Loss Prevention Software-Find PII On Computer.url](#)

## **MODULE 9**

### **MOBILE DEVICE SECURITY**

#### **REVIEW**

[OMB Memo 06-16: Protection Sensitive Information-Removed From/Accessed From Outside Agency.pdf](#)

[NIST SP 800-124: Guidelines on Cell Phone and PDA Security.pdf](#)

[Managing Mobile Computing Risks.pdf](#)

[Laptop Security Guidance Brochure.doc](#)

#### **TRAINING**

[Portable Electronic Devices and Removable Storage Media Training.url](#)

[Traveling Overseas With Mobile Phones, Laptops, PDAs, & Other Electronic Devices.pdf](#)

#### **REFERENCE**

##### **MOBILE DEVICE THEFT AND RECOVERY / DATA PROTECTION**

[Mobile Device Recovery Software.url](#)

[Laptop Alarm: Sets Off An Alarm Whenever It Detects A Possible Theft.url](#) (Free Software)

[Doberman Laptop Defender Portable USB Computer Alarm.pdf](#)

[How to Stop Laptop Theft.url](#)

[Have Your Lost USB Drive Ask For Help.url](#)

##### **DISK ENCRYPTION SOFTWARE/HARDWARE**

[Windows Encrypting File System-Controlling Using Group Policy.pdf](#)

[Windows 7 BitLocker Encryption Vs. EFS.url](#)

[Windows 7 Encryption.url](#)

[Windows 7 BitLocker Drive Encryption Deployment Guide.url](#)

[Windows Vista BitLocker Drive Encryption.url](#)

[Windows Vista BitLocker Drive Encryption Configuration Guide.url](#)

[Disk Encryption Applications Put A Lock On Data.pdf](#)

[Hard Drives With Built In Encryption.url](#)

[Encrypt Them All.pdf](#)  
[USB Flash Drive Encryption Software.url](#)

## **MODULE 10**

### **SECURITY SERVICES AND PRODUCT ACQUISITION**

#### **REVIEW**

[NIST SP 800-100: Chapter 12 Security Services and Products Acquisition.pdf](#)  
[Dept. Of Commerce Training Video: Effectively Integrating IT Security Into The Acquisition Process.url](#)  
[Dept. Of Commerce Training Material: Effectively Integrating IT Security into The Acquisition Process.url](#)

#### **REFERENCE**

[NIST SP 800-35: Guide To Information Technology Security Services.pdf](#)  
[NIST SP 800-36: Guide To Selecting Information Technology Security Products.pdf](#)  
[NIST: Software Assurance In Acquisition Planning, Contracting, Implementation And Acceptance Phases.pdf](#)

## **MODULE 11**

### **SECURITY POLICIES AND PROCEDURES**

#### **REVIEW**

[Presentation: Security Policies And Procedures.pdf](#)  
[NIST SP 800-14: Security Policy Overview.pdf](#)  
[CERT Presentation: Policy Formulation And Implementation.pdf](#)  
[Dept. of Justice IT Security Guide: Formalize IT Security Policies.pdf](#)

#### **REFERENCE**

##### **POLICY AND PROCEDURES EXAMPLES**

[Federal Agency Security Practices.url](#)  
[National Science Foundation's USAP Information Security Policies And Instructions.url](#)  
[Recommended Security Policies.pdf](#)  
[Practical IT Policies And Procedures Examples.pdf](#)  
[The SANS Security Policy Project.url](#)  
[Policy for Personal Use Of Information Technology Resources.pdf](#)  
[Limited Personal Use Of Government Office Equipment And IT Equipment.pdf](#)  
[USDA: Internet Usage And E-Mail Guidelines.pdf](#)  
[EPA: Privacy Policy.pdf](#)

##### **SOCIAL NETWORKING GUIDANCE**

[GSA: Guidance For Web 2.0 / Social Networking Websites \(Policies & Handbook\).url](#)  
[CIO Council: Cyber Guidelines For Web 2.0.url](#)  
[EPA: Guidance Online Using Social Media.url](#)

## **MODULE 12**

### **INFORMATION SECURITY AWARENESS / EDUCATION / TRAINING**

#### **REVIEW**

[Presentation: Information Security Awareness-Training-Education.pdf](#)  
[NIST SP 800-100: Chapter 4 Security Awareness Training.pdf](#)  
[NIST Presentation: Building An IT Security Awareness Program.pdf](#)

#### **MANDATORY TRAINING FOR FEDERAL GOVERNMENT, DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY**

[Federal Information Systems Security Awareness Training.url](#)  
[Intelligence Community Information Assurance Awareness Training.url](#)  
[DOD Information Assurance Awareness Training.url](#)  
[DOD Training: Personally Identifiable Information/PII.url](#)

#### **REFERENCE**

[NIST SP 800-50: Building An Information Technology Security Awareness and Training Program.pdf](#)  
[NIST SP 800-16: Information Security Training Requirements: A Role And Performance Based Model.pdf](#)  
[Security Awareness Improving Security Inside-Out.pdf](#)

## INFORMATION SECURITY AND PRIVACY AWARENESS AND TRAINING MATERIAL

[Overview of AggregationThreat.pdf](#)

[Overview of Elicitation Threat.pdf](#)

[Overview of Social Engineering Threats.pdf](#)

[Laptop Security Guidance Brochure.doc](#)

[Messaging-Mobile Security And Privacy Overview.pdf](#)

[A Messy Desk Is A Vulnerable Desk-Security Risk.pdf](#)

[DISA Information Assurance Awareness-Online Training.url](#)

[DOD Free IA Training-Awareness Products Descriptions.pdf](#)

[DOD Free IA Training-Awareness Products Order Form.doc](#)

## INFORMATION SECURITY AWARENESS POSTERS

[DNI National Counterintelligence Executive \(NCIX\) Posters.url](#)

[DIA Security Posters.zip](#)

[DISA IA Awareness Posters.url](#)

[Department of Homeland Security Posters.url](#)

[Computer Security Awareness Posters.url](#) (Bottom Of Page)

[Free Security Awareness Posters And Resources-1.url](#)

[Free Security Awareness Posters And Resources-2.url](#)

[Security Awareness Posters.zip](#) (Right Click-Save Target As-Save Location)

[SCIF Security Posters.ppt](#)

## MODULE 13

### ACCESS CONTROL LIFECYCLE

### IDENTIFICATION / AUTHENTICATION / AUTHORIZATION / TERMINATION

#### REVIEW

[Presentation: Access Control-Identification-Authentication.pdf](#)

[Access Controls Lifecycle Checklist.pdf](#)

[Access Control In-Depth.pdf](#)

#### REFERENCE

[Network Access Request And Authorization Form.pdf](#)

[Two Factor Authentication Options.pdf](#)

#### E-AUTHENTICATION FOR WEB BASED APPLICATIONS

[OMB E-Authentication Guidance For Federal Agencies Overview.pdf](#)

[OMB Memo 04-04: E-Authentication For Federal Agencies.pdf](#)

[NIST SP 800-63: Electronic Authentication Guidelines For Remote Authentication Of Users.pdf](#)

[IDManagement.Gov Webpage.url](#)

[IDManagement.Gov Electronic Risk And Requirements Assessment Tool.url](#)

#### MICROSOFT WINDOWS AUTHENTICATION

[Windows Login Controls.pdf](#)

[UserLock Software- Secures Access To Windows Networks By Restricting Simultaneous/Concurrent Logins.url](#)

## MODULE 14

### GENERAL USERS SECURITY REQUIREMENTS

### RULES OF BEHAVIOR FOR COMPUTER SYSTEMS / NETWORK ACCESS

### INFORMATION SYSTEMS SECURITY BRIEFINGS

#### REVIEW

[Presentation: Generals Users Security Requirements.pdf](#)

[NIST SP 800-100: Rules Of Behavior Overview.pdf](#)

[Rules Of Behavior And Disciplinary Actions Overview.pdf](#)

#### REFERENCE

#### INFORMATION SECURITY/ INFORMATION SYSTEMS SECURITY BRIEFINGS

[DOD/IC Rules Of Behavior Briefing And Acknowledgement Agreement.doc](#) (Use For New Hire Briefings & Security Education Awareness)

[SCIF Security Briefing.ppt](#)

[SCIF Information Security/Information Systems Security Policies-Procedures-Guidelines.pdf](#)  
[SCIF Security Violation Warning Notice.doc](#)  
[FBI: Rules of Behavior-Acknowledgement Agreement.pdf](#)  
[USCG: Information Systems User Briefing And Acknowledgement Agreement.pdf](#)  
[HHS: Rules of Behavior-Acknowledge Agreement.pdf](#)  
[NSF: User Information Security Awareness Booklet/Rules Of Behavior.pdf](#)  
[NSF: Information Security Policies Acknowledgement.pdf](#)  
[USDA: Internet Usage And E-Mail Guidelines.pdf](#)

## **MODULE 15**

### **PRIVILEGED USERS SECURITY REQUIREMENTS**

#### **NETWORK AND SYSTEM ADMINISTRATORS**

##### **REVIEW**

[Presentation: Privileged Users Security Requirements.pdf](#)  
[Privileged Users: Network And Systems Administrators Security Responsibilities Overview.pdf](#)  
[Privileged Users: Network And Systems Administrators Security Responsibilities Acknowledge Agreement.pdf](#)

##### **REFERENCE**

[Information Systems And Networks Standard Operating Procedures For Administrators.pdf](#)  
[DOD 8570.1 Privileged User Access Agreement-Acknowledge Of Responsibilities.pdf](#)  
[JDCSISSS SCI Systems Administrator Requirements And Acknowledgement Form.pdf](#)  
[Microsoft Administrator Accounts Security Planning Guide.pdf](#)

## **MODULE 16**

### **RISK MANAGEMENT / CONTINUOUS MONITORING**

##### **REVIEW**

##### **CONTINUOUS MONITORING OVERVIEW**

[Presentation: Continuous Monitoring Program Overview.pdf](#)  
[Presentation: Continuous Monitoring Program.pdf \(From Compliance to Risk Management\)](#)  
[CNSS Policy No. 22: Information Assurance Risk Management Policy For National Security Systems.pdf](#)  
[NIST FAQ'S On Continuous Monitoring.pdf](#)  
[Continuous Monitoring Plan Template.doc](#)

##### **REFERENCE**

##### **RISK MANAGEMENT OVERVIEW**

[NIST Risk Management Framework.pdf](#)  
[NIST SP 800-100: Chapter 10 Risk Management.pdf](#)  
[NIST Risk Management Framework / Quick Start Guides.url](#)  
[Presentation: CERT Assets and Risk Management.pdf](#)  
[Presentation: Risk Management.pdf](#)  
[Why You Need To Conduct A Risk Assessment.pdf](#)  
[Understanding Assets And Risk-Video Based.url](#)  
[Risk Assessments-Video Based.url](#)

##### **RISK ASSESSMENT AND SECURITY INSPECTION CHECKLISTS**

[NIST SP 800-53: Security Controls Assessment Form.pdf](#)  
[Dept. Of Justice IT Security: Risk Assessment Worksheets And Questions.pdf](#)  
[Dept. Of Justice IT Security Risk Assessment Tool.xls](#)  
[Information System Security Risk Assessment Questionnaire And Checklist.pdf](#)  
[CMS Threat Identification Resource.pdf](#)  
[Threat Identification Workbook For Software Applications.doc](#)  
[Information Security Program Inspection Topics For Review.pdf](#)  
[Information Security Inspection And Assessment Checklists.xls](#)

##### **RISK MANAGEMENT REFERENCES**

[NIST SP 800-30: Risk Management Guide For IT Systems.pdf](#)  
[NIST SP 800-39: Managing Risk From Information Systems.pdf](#)  
[CMS Information Security Risk Assessment Methodology.pdf](#)  
[Dept Of Justice IT Security: How To Assess Risk And Establish Effective Policies.pdf](#)

[Internal Audit Of Organization's Risk Management Program And Processes.pdf](#)  
[Microsoft Security Risk Management Guide.url](#)  
[State Dept. Improves Security, While Cutting Costs With Continuous Monitoring.url](#)  
**RISK MANAGEMENT CONTINUOUS MONITORING TOOLS**  
[Xacta IA Manager.url](#)

## **MODULE 17**

### **CERTIFICATION AND ACCREDITATION / C&A**

#### **REVIEW**

##### **OVERVIEW OF CERTIFICATION AND ACCREDITATION**

[NIST Presentation: Risk Management / Certification And Accreditation.pdf](#)

**NEW-** [NIST SP 800-37 Rev. 1-- DRAFT Guide for Applying The Risk Management Framework To Federal Information Systems.pdf](#)

**OLD-** [NIST SP 800-37: Guide For Security Certification-Accreditation Of Federal Information Systems.pdf](#)

[NIST SP 800-37: Certification And Accreditation Process Chart.pdf](#)

[NIST SP 800-100: Chapter 11 Certification And Accreditation.pdf](#)

[NIST SP 800-100: Chapter 3 System Development Life Cycle.pdf](#)

#### **REFERENCE**

[Department of Energy Certification-Accreditation Guidance.pdf](#)

[CMS Certification And Accreditation Procedures.pdf](#)

[CMS Certification-Accreditation Process Supporting Documentation.doc](#)

#### **DNI TEMPLATES**

[DNI C&A Documents Library.url](#) (Requires Intelink & Passport Account)

[Security Assessment Report Template.doc](#)

[Continuous Monitoring Plan Template.doc](#)

[POA&M Template.doc](#)

#### **SYSTEM SECURITY PLANS / SSP'S**

[NIST SP 800-18: Guide For Developing Security Plans For Federal Information Systems.pdf](#)

[Housing And Urban Development SSP Template.doc](#)

[CMS SSP Template.doc](#)

[CDC SSP Template.doc](#)

[System Security Plan Checklist.xls](#)

[System Security Plan Checklist.pdf](#)

#### **SECURITY TEST AND EVALUATION / ST&E**

[Presentation: Systems Security Certification Testing.pdf](#)

[HHS Security Test And Evaluation Guide.pdf](#)

[CMS Reporting Standard for Information Security Testing.pdf](#)

[CMS Information Security Testing Approach.pdf](#)

[Security Test And Evaluation Plan Template.doc](#)

#### **SYSTEMS DEVELOPMENT LIFE CYCLE**

[NIST SP 800-64: Security Considerations In The Systems Development Life Cycle.pdf](#)

[NIST SP 800-64: Chapter 3 Incorporating Security Into The Systems Development Life Cycle.pdf](#)

## **MODULE 18**

### **SECURITY VULNERABILITY TESTING OF INFORMATION SYSTEMS AND NETWORKS**

### **SECURITY VULNERABILITY DATABASES AND ALERTS**

#### **REVIEW**

[NIST SP 800-115: Overview To Information Security Testing.pdf](#)

[NIST SP 800-15: Overview Penetration Testing.pdf](#)

[NIST SP 800-40 Chapter 2: Creating A Patch And Vulnerability Management Program.pdf](#)

[CERT Presentation: Best Practices For Security Vulnerability Assessment Tools.url](#)

[Vulnerability Management For Dummies.pdf](#)

#### **WEB APPLICATION THREATS AND VULNERABILITIES**

[SANS Report: The Top Cyber Security Risks.url \(9/2009\)](#)

[FTC Warns of Improper Release Of Sensitive Consumer Data On P2P File-Sharing Networks.pdf](#)

[Peer To Peer Network Data Breaches.pdf](#)

## **REFERENCE**

### **SECURITY TESTING GUIDANCE**

[NIST SP 800-115: Technical Guide For Information System Security Testing.pdf](#)

[NIST SP 800-40: Creating A Patch And Vulnerability Management Program.pdf](#)

[NIST Information Systems Security Testing Rules of Engagement.pdf](#)

[CMS Information Security Testing Approach.pdf](#)

[CMS Reporting Standard For Information Security Testing.pdf](#)

[Comparison of Security Testing Techniques.pdf](#)

[Penetration Testing Reference Manual .pdf](#)

[Guidelines For Developing Penetration Testing Rules Of Behavior.pdf](#)

[ISSM Approval To Conduct Network Testing.pdf](#)

### **SECURITY VULNERABILITY DATABASES**

[National Vulnerability Database Search.url](#)

[US-CERT Vulnerability Notes Database.url](#)

### **SECURITY ALERTS**

[US-CERT Federal Knowledge Base System For Vulnerabilities Alerts.url](#)

[US-CERT Technical Cyber Security Alerts.url](#)

[KBAlertz.com - Knowledge Base Alerts.url](#)

### **COMMERCIAL SECURITY VULNERABILITY TESTING TOOLS**

[Core Impact Security Penetration Testing Tool.url](#)

[eEye Retina Vulnerability Scanner.url](#)

[GFI LANGuard Vulnerability Manager.url](#)

### **FREE SECURITY VULNERABILITY TESTING TOOLS**

[The Essential Guide to Vulnerability Scanning.url](#)

[Security Tools To Assess Web And Network Vulnerabilities.url](#)

[Security Tools Used By The Attacker / Web Application Penetration Testers.url](#)

[Top 100 Network Security Tools.url](#)

[Open Source Monitoring Tools.url](#)

[Rogue Scanner Network Discovery And Device Classification.url](#)

[Metasploit Vulnerability Finder Overview.url](#)

[Metasploit Vulnerability Finder Download.url](#)

[Nessus Vulnerability Scanner.url](#)

[NMAP Network Mapper.url](#)

[NMAP Unit Graphical Front End For NMAP.url](#)

[NetBrute Scanner.url](#) (Check For Open TCP/IP Ports, Windows File & Print Sharing Resources, Open Web Directories)

[BackTrack Security Testing CD.url](#)

[Samurai Web Site Testing CD.url](#)

### **SECURITY VULNERABILITY TESTING TOOLS TRAINING / HOW TO**

[Basic NMAP Usage.url](#)

[NMAP Technical Manual.url](#)

[NMAP Port Scanning.url](#)

[Nessus 3 Tutorial.url](#)

[Nessus 3 Demo.url](#)

[Demonstrations Of Security Vulnerability Tools.url](#)

[Ethical Hacking & Penetration Testing Tutorials.url](#)

[Using Packet Analysis For Network Troubleshooting.pdf](#)

### **MICROSOFT WINDOWS AND UNIX SECURITY COMPLIANCE VERIFICATION TOOLS**

**[WASSP AND SECSCN NIST / DCID 6/3 SECURITY COMPLIANCE TESTING TOOLS OVERVIEW \(Provided By SSO Navy\)](#)**

[WASSP And SECSCN Security Compliance Scanners Overview.pdf](#)

[Presentation: WASSP And SECSCN Security Compliance Scanners.pdf](#)

[WASSP Example Report.pdf](#)

### **WASSP DOWNLOAD**

[WASSP Version 4.4 Download Link.url](#) (Requires Intelink & PassPort Account)

[WASSP Version 4.4 Download File.zip](#) (16MB) (Then Burn ISO Image To CD)

### **SECSCN DOWNLOAD**

[SECSCN Version 4.4 Download Link.url](#) (Requires Intelink & PassPort Account)

[SECSCN Version 4.4 Download File.zip](#) (5MB) (Then Burn ISO Image To CD)

## **MICROSOFT SECURITY BASELINE ANALYZER FOR MICROSOFT WINDOWS**

[How To Use The Microsoft Baseline Security Analyzer.url](#)

[Microsoft Baseline Security Analyzer.url](#)

## **OTHER WINDOWS SECURITY COMPLIANCE TESTING TOOLS**

[CIS Compliance Advisor - Free Audit Tool By Belarc.url](#) (Checks Compliance With Center for Internet Security Benchmarks)

## **MICROSOFT SYSINTERNALS SECURITY TOOLS**

### **DESCRIPTION:**

Microsoft Sysinternals Utilities Will Help You Manage, Troubleshoot And Diagnose The Windows Operating Systems And Applications Sysinternals Utilities- File And Disk, Networking, Windows Processes, Security, Systems Information

[Microsoft Sysinternals Utilities.url](#)

## **PASSWORD GUIDANCE / PASSWORD SECURITY TESTING TOOLS**

[NIST SP 800-118: Guide to Enterprise Password Management.pdf](#)

[Microsoft Password Strength Verification Tool.url](#)

[Sniffing Out Passwords On Websites.pdf](#)

[Cain & Abel Password Recovery Tool For Microsoft Operating Systems.url](#)

## **NETWORK TRAFFIC ANALYSIS TOOLS**

[Solarwinds Real-Time Network Traffic Analyzer Overview.url](#)

[Solarwinds Real-Time Network Traffic Analyzer.url](#)

[NetWitness Investigator Packet Capture And Analysis Tool Overview.url](#)

[NetWitness Investigator Download.url](#)

[NetworkMiner Network Forensic Analysis / Packet Analyzer Tool Overview.pdf](#) (Excellent Sniffer Tool-No Install Required)

[NetworkMiner Network Forensic Analysis / Packet Analyzer Tool.url](#)

[Colasoft Packet Player.url](#) (Open Captured Packet Trace Files And Play Them Back In The Network)

## **WIRELESS SECURITY TESTING TOOLS**

[NetStumbler: Wireless Networking Detection Tool.url](#) (Download)

[Earth Stumbler.url](#) (Earth Stumbler Is A Program To Import GPS-Tagged NetStumbler Information Into Google Earth)

[WiFi Hopper Network Discovery And Site Survey Tool.url](#)

[Wireless NetView.url](#)

[InSSIDer WiFi Scanner.url](#)

[AirGrab WiFi Radar.url](#) (Display Information About Apple Airport Base Stations And Other WiFi Access Points)

[KisMAC WiFi Network Scanner Software For Mac OS X.url](#)

[iStumbler WiFi Discovery Tool For Mac OS X.url](#)

[Wireshark Network Protocol Analyzer.url](#)

[WireShark: Basic Network Application Troubleshooting.url](#)

[AirSnare: Monitors Wireless Network Traffic For Unfriendly MAC Addresses.url](#)

[Bluetooth View: Detect Bluetooth Devices.url](#)

## **WEB APPLICATION SECURITY TESTING TOOLS**

[Microsoft PReFast Code Scanning Security Tool.url](#) (Free)

[Acunetix Free Cross Site Scripting Security Scanner.url](#)

[SQL Injection Attacks-Testing Tools.url](#)

[Finding SQL Injection With Scrawl.url](#)

[IBM Rational AppScan.url](#)

## **WEB APPLICATION TRAFFIC MONITORING AND REPORTING TOOLS**

[Tiversa P2P Intelligence Experts.url](#)

[Facetime: Monitoring / Reporting Of Web Browsing, Instant Messaging And P2P Traffic.url](#)

[Sophos Web Application Discovery Tool For Networks.url](#)

[Sophos Web Application Discovery Tool For Networks Overview.pdf](#)

[FTP File Transfer Analyzer.url](#) (Free Tool)

## **GOOGLE SECURITY TESTING TOOLS**

[Google Hacking By Johnny Long.url](#)

[Google Hacking for Penetration Testers.pdf](#)

[Google Hacker's Guide.pdf](#)

[Google Hacking Mini-Guide Basic Search Techniques.url](#)

[Using Google As A Vulnerability Scanner.pdf](#)

## **INTRUSION DETECTION SYSTEMS / IDS**

[Knoppix-NSM Live CD.url](#)

[Knoppix-NSM Live CD Review.pdf](#)

[Snort Intrusion Detection System.url](#)

[Snort Intrusion Detection and Prevention Guide.url](#)

## **MODULE 19**

### **CONFIGURATION MANAGEMENT**

#### **REVIEW**

[NIST SP 800-100: Chapter 14 Configuration Management.pdf](#)

[Presentation: Configuration Management.pdf](#)

[Un-Planned And Un-Controlled Changes To IT Networks And Computing Systems Infrastructures.pdf](#)

[Configuration Management Examples Of Security Significant Changes.pdf](#)

#### **REFERENCE**

##### **CONFIGURATION MANAGEMENT PLANS AND POLICIES**

[NASA Configuration Management Plan.pdf](#)

[POL-0005 Configuration Change Management Policy.pdf](#)

[POL-0005 Configuration Change Request Form.pdf](#)

[Configuration Management Hardware-Software Implementation Checklist.pdf](#)

[POL-0013 Information Systems Maintenance Policy.pdf](#)

[POL-0013 Information Systems-Network Equipment Maintenance Log.pdf](#)

##### **CHANGE MANAGEMENT SOFTWARE**

[Xacta IA Manager Continuous Assessment.url](#)

[ECORA Configuration and Change Management Software.url](#)

[Belarc BelManage Enterprise Configuration Management Software.url](#)

[Tripwire Configuration Change Management Software.url](#)

[Open Source Tripwire For Linux And Unix.url](#)

[InstallWatch Change Mangement Software Overview.pdf](#)

[InstallWatch Change Mangement Software.url](#)

[Windows XP Change Analysis Diagnostic Tool.url](#)

[Whats Running System Information Utility.url](#)

##### **INVENTORY MANAGEMENT SOFTWARE**

[Lansweeper Hardware/Software Inventory For Windows Networks.url](#)

##### **CONFIGURATION MANAGEMENT RESOURCES**

[The Administrator Shortcut Guide to Configuration Management For The Windows Enterprise.url](#)

[The Definitive Guide To Enterprise Change Management.url](#)

[The Definitive Guide To Enterprise Network Configuration And Change Management.url](#)

## **MODULE 20**

### **PLAN OF ACTION AND MILESTONES / POA&MS**

#### **REVIEW**

[Presentation: Plan Of Action And Milestones-POA&MS.pdf](#)

[OMB Guidelines For Preparing And Submitting Plan Of Actions And Milestones.pdf](#)

[Example POA&M Report.pdf](#)

[POA&M Chart.pdf](#)

#### **REFERENCE**

[Dept. Of Energy-Plan Of Actions And Milestones.pdf](#)

[HHS CMS POA&M Guidelines.pdf](#)

## **MODULE 21**

### **INFORMATION SYSTEMS AUDITING / LOGGING, MONITORING AND REPORTING**

#### **REVIEW**

[Presentation: Information Systems Security Audit Requirements Overview.pdf](#)

[Windows Operating System Audit Policy Overview.pdf](#)

[Windows Operating System Event Logs Overview.pdf](#)

[Introduction To Logging, Monitoring And Reporting Of IT Security Controls And Processes.pdf](#)

#### **REFERENCE**

[NIST SP 800-92: Guide To Computer Security Log Management.pdf](#)

##### **WINDOWS OPERATING SYSTEM AUDITING**

[Microsoft Events And Errors Message Center Advanced Search.url](#)  
[Microsoft Security Monitoring and Attack Detection Planning Guide.pdf](#)  
[Windows 2003 Security Guide-Chapter 4 Audit Policy.pdf](#)  
[Windows Operating System Auditing Overview.pdf](#)  
[Windows Operating System Event Logs Overview.pdf](#)  
[Windows Event IDs For Windows Server 2008 And Vista.url](#)  
[Deploying Windows Auditing Settings And Reporting What Is Configured.url](#)

#### **WINDOWS OPERATING SYSTEM AUDITING TOOLS**

[Microsoft System Center Operations Manager 2007.url](#)  
[DumpSec Security Auditing Program For Microsoft Windows NT/XP/2000/2003.url](#)  
[LogLogic.url](#)  
[Event Log Explorer.url](#)

#### **WINDOWS OPERATING SYSTEM / ACTIVE DIRECTORY AUDITING**

[Windows & Active Directory Auditing.url](#)  
[How To Enable Active Directory Access Auditing In Windows 2000.url](#)  
[How To Audit Active Directory Objects In Windows 2000.url](#)  
[How To Audit Active Directory Objects In Windows Server 2003.url](#)  
[Windows Server 2008: Active Directory Auditing.url](#)  
[Understanding Active Directory Auditing in Windows Server 2008.pdf](#)

#### **WINDOWS OPERATING SYSTEM / ACTIVE DIRECTORY AUDITING TOOLS**

[Change Auditor For Active Directory.url](#)  
[Active Directory Reporter.url](#)  
[NetWrix Active Directory Change Reporter.url](#)  
[Active Directory Cleaner.url](#)

#### **LINUX SECURITY**

[Linux Security Quick Reference Guide.pdf](#)  
[Linux Security Administrator's Guide: User, System, and Process Accounting.url](#)  
[Linux Security Administrator's Guide: Intrusion Detection.url](#)

#### **USB PORT AUDITING**

[USBDeview - View Installed-Previously Connected USB Devices On System.url](#)

#### **DATABASE AUDITING**

[Oracle Audit Vault.url](#) (Collection, Monitoring And Reporting For Microsoft SQL Server, IBM DB2, Sybase Databases)  
[Guardium Database Security And Monitoring.url](#)  
[Database Auditing Traditional Vs Non-Traditional.pdf](#)

#### **MICROSOFT EXCHANGE SERVER AUDITING**

[DigiScope Exchange Server Investigation Tool.url](#)

#### **E-MAIL CONTENT FILTERING**

[Axway MailGate.url](#)  
[Clearwith MIMESeeper For SMTP.url](#)  
[Clearswift Contentsafe.url](#)

#### **DNS CONTENT FILTERING**

[OpenDNS Web Content Filtering Overview.url](#) (Free)  
[OpenDNS Home Page.url](#)

#### **ROUTER SECURITY AUDIT LOGS**

[Cisco Router Security Audit Logs.url](#)

#### **INTRUSION DETECTION SYSTEMS**

[NIST SP 800-94: Guide to Intrusion Detection And Prevention Systems.pdf](#)

#### **EMPLOYEE AUDITING, MONITORING AND INVESTIGATIONS**

[Spectorsoft Employee Monitoring Software.url](#)  
[Raytheon SureView.url](#)

## **MODULE 22**

## **INCIDENT RESPONSE AND REPORTING**

### **REVIEW**

[NIST SP 800-100: Chapter 13 Incident Response.pdf](#)  
[Presentation: Incident Response And Reporting.pdf](#)  
[POL-0002 Computer Incident Reporting Policy.pdf](#)  
[POL-0002 FORM-Network-Computer Incident Report.pdf](#)  
[POL-0014 Release Of Information To The Public-Media.pdf](#)

## **REFERENCE**

[NIST SP 800-61: Computer Security Incident Handling.pdf](#)

## **COMPUTER FORENSICS**

[NIST SP 800-86: Guide To Integrating Forensics Techniques Into Incident Response.pdf](#)

[Fundamental Computer Investigation Guide for Windows.url](#)

## **SECURITY INCIDENTS AND VIOLATIONS**

[Microsoft: Responding To IT Security Incidents.url](#)

[Information Security-Systems Security Violation Notice.pdf](#)

[Cyber Security Incident Report.pdf](#)

## **MALICIOUS CODE RISKS AND MITIGATION**

[Presentation: Malicious Code Risks And Mitigation.pdf](#)

[NIST SP 800-83: Guide To Malware Incident Prevention and Handling.pdf](#)

[Microsoft Antivirus Defense-In-Depth Guide.pdf](#)

[BotHunter Software Detects Malware On Networks.url](#)

[BotHunter Malware Detection Software Download.url](#)

## **COMPUTER SECURITY INCIDENT RESPONSE TEAMS**

[CMU CERT: Creating a Computer Security Incident Response Team A Process for Getting Started.url](#)

[CMU CERT: Handbook For Computer Security Incident Response Teams.pdf](#)

[CSIRT: Step By Step Approach On How To Set Up A CSIRT.pdf](#)

[Computer Security Incident Response Team FAQ.url](#)

## **FEDERAL GOVERNMENT INCIDENT REPORTING**

[Dept. Of Homeland Security / US-CERT.url](#)

[US-CERT Incident Reporting Guidelines.url](#)

[US-CERT Incident Reporting System.url](#)

[GFIRST-Government Forum of Incident Response and Security Teams.url](#)

## **MODULE 23**

### **DOCUMENT SECURITY**

#### **METADATA PROBLEMS IN MICROSOFT OFFICE DOCUMENTS / PDF FILES**

## **REVIEW**

[Presentation: SRS Electronic Document Security Introduction.pps](#)

[Presentation: SRS TopTen Hidden Data Issues.wmv](#)

[Metadata Risks: Microsoft Office And Adobe PDF Documents.pdf](#)

## **METADATA PROBLEMS IN THE NEWS**

[Published Incidents Involving Hidden Data.url](#)

[Pentagon Document Revealed Un-Classified Highly Sensitive Information.pdf](#)

[Agencies Accidental Release Of Sensitive Information Using Office Applications.pdf](#)

## **REFERENCE**

[Establishing An Electronic Document Security Program.pdf](#)

## **US GOVERNMENT POLICIES AND REGULATIONS**

[Protection Of Sensitive Personal Information.url](#)

## **SOFTWARE TO REMOVE METADATA**

[Document Detective Metadata Removal Software.url](#) (Reviewed And Recommended)

IC Clear (Located On JWICS: <http://icclear.csp.ic.gov/MainPage.htm>)

[Protect Your Privacy When Uploading Photos.url](#)

## **REDACTION OF INFORMATION FROM DOCUMENTS**

[NSA: How To Safely Publish Sanitized Reports Converted From A Word Document To PDF Document.pdf](#)

[Adobe: Redaction of Confidential Information In Electronic Documents.pdf](#)

## **TRAINING ON MICROSOFT DOCUMENT SECURITY**

[Protect Word Documents.url](#)

[Audio Course: Revise Documents With Track Changes And Comments.url](#)

[Quick Reference Card: Revise Documents With Track Changes And Comments.url](#)

[Help Secure And Protect Data In Excel.url](#)

[Microsoft Office Security Basics.url](#)

[Microsoft References For Office Document Security.pdf](#)

[Microsoft Office: Help And How To.url](#)

## **MODULE 24**

### **THREATS AND VULNERABILITIES**

#### **REVIEW**

[Presentation: Overview Of Threats.pdf](#)

[CERT: Threats, Vulnerabilities And Attacks Affecting Information Systems.pdf](#)

[US CERT: Common Sense Guide To Prevention-Detection Of Insider Threats.pdf](#)

#### **REFERENCE**

[Inside Job: 8 Companies That Got Burned by Rogue IT Workers.url](#)

[Air Force Presentation: Threats From Electronic Devices.pdf](#)

[Technology Threats To IT Systems And Data.pdf](#)

[10 Top Spy Gadgets.url](#)

[Mossad Reappearing Ink Pen.url](#)

[Steganography Overview-More Than Meets The Eye.pdf](#)

[Steganography Demo.url](#)

[New Google Desktop Search Raises Privacy Concerns.pdf](#)

[Preventing Data Leakage Through E-Mail And Instant Messaging.pdf](#)

[A Messy Desk Is A Vulnerable Desk-Security Risk.pdf](#)

[USB Threats-USB Hacks.pdf](#)

## **MODULE 25**

### **ELECTRONIC COMPUTER STORAGE MEDIA**

#### **CLEARING / SANITIZING / DESTRUCTION**

#### **REVIEW**

[Presentation: Clearing, Sanitizing, Destruction Of Computer Media.pdf](#)

[NIST SP 800-88: Guidelines For Media Sanitization.pdf](#)

[POL-0004 Computer Media Clearing-Sanitization-Destruction Policy.pdf](#)

[POL-0004 Computer Media Deguassed-Destruction Form.pdf](#)

#### **REFERENCE**

##### **DISK WIPING SOFTWARE**

[Active Kill Disk Hard Drives Eraser.url](#)

[BCWipe For Windows.url](#)

[BCWipePD.url](#)

[Darik's Boot and Nuke.url](#)

##### **CLEARING, SANITIZATION AND DESTRUCTION OF CLASSIFIED / SENSITIVE DATA**

[DSS Procedures For Clearing-Sanitization Of Electronic Media.pdf](#)

[DSS Clearing-Sanitization Matrix.pdf](#)

[DSS Blackberry Clearing Procedure For Devices Containing Secret Data.pdf](#)

##### **NSA GUIDANCE**

[NSA-CSS Storage Device Declassification Manual.pdf](#)

[NSA Guidance For Downgrading of Hard Drives.pdf](#)

[NSA Procedures For Destruction Of Classified Material At NSA/CMC Facility.url](#)

[NSA Classified Hard Drive Destruction NSA/CMC Facility Contact Info.pdf](#)

##### **REPORTS ON DATA PROTECTION OF USED STORAGE MEDIA**

[Data Protection of Used Storage Media.pdf](#)

## **MODULE 26**

### **CONTINUITY OF OPERATIONS PLANNING / COOP**

#### **IT CONTINUITY PLANNING**

#### **DISASTER RECOVERY PLANNING**

#### **REVIEW**

[Presentation: FEMA COOP Awareness Training.pdf](#)

[NIST SP 800-100: Chapter 9 Information Technology Contingency Planning.pdf](#)

[FEMA COOP Overview.pdf](#)

## **REFERENCE**

### **TRAINING**

[FEMA Continuity of Operations Training Class.pdf](#)

[IS-546 Continuity of Operations \(COOP\) Awareness Course.url](#)

[IS-547 Introduction to Continuity of Operations \(COOP\).url](#)

[NARA Vital Records Presentation.ppt](#)

### **BUSINESS CONTINUITY MANAGEMENT**

[Guide To Business Continuity Management.pdf](#)

### **INFORMATION SYSTEMS CONTINGENCY PLANNING**

[NIST SP 800-34: Contingency Planning Guide For Information Technology Systems.pdf](#)

[Information Systems Contingency Plan Template.pdf](#)

[Contingency Plan Audit Checklist For High Availability Information Systems.pdf](#)

### **BUSINESS IMPACT ANALYSIS / DISASTER RECOVERY PLANS**

[Business Impact Analysis.pdf](#)

[Information Technology Disaster Recovery Plan.pdf](#)

### **COOP TEMPLATES**

[FEMA COOP Plan Template Instructions.pdf](#)

[FEMA COOP Template.pdf](#)

[Facility-Systems Contingency Plan Template.pdf](#)

### **ALTERNATE FACILITIES SECURITY AND ASSESSMENTS**

[19 Ways To Build Physical Security Into A Data Center.url](#)

[How to Design a Secure Facility.url](#)

[GSA Securing Alternate Facilities Worksheet.pdf](#)

[Alternate Facility Assessment.pdf](#)

## **MODULE 27**

### **REMOTE ACCESS TO AGENCY INFORMATION SYSTEMS AND DATA**

#### **TELEWORKING**

### **REVIEW**

[OMB Memo 06-16: Protection Sensitive Information-Removed From/Accessed From Outside Agency.pdf](#)

[OMB E-Authentication Guidance For Federal Agencies Overview.pdf](#)

## **REFERENCE**

### **E-AUTHENTICATION FOR WEB BASED APPLICATIONS**

[OMB Memo 04-04: E-Authentication For Federal Agencies.pdf](#)

[Electronic Risk And Requirements Assessment Tool For E-Authentication.url](#)

[NIST SP 800-63: Electronic Authentication Guidelines For Remote Authentication Of Users.pdf](#)

### **TELEWORKING**

[Telework.Gov Website For Government Teleworkers And Managers.url](#)

[Guide To Telework In The Federal Government.pdf](#)

### **BROADBAND COMMUNICATIONS SECURITY**

[NIST SP 800-46: Guide To Enterprise Telework And Remote Access Security.pdf](#)

[NIST SP 800-113: Guide To SSL VPNS.pdf](#)

## **MODULE 28**

### **FREE COMPUTER SECURITY / INFOSEC TRAINING**

#### **INFORMATION SYSTEMS SECURITY TRAINING AND EDUCATION**

[CISSP Essentials Security School.url](#) (Each Of The 10 Lessons Includes A 45 Minute Video Presentation, Article And Quiz)

[CISSP Handbook of Information Security Management.url](#)

[CISSP Training.url](#)

[InfoWorld's Security Boot Camp.url](#)

[SearchSecurity.com: Security School On-Line Course Catalog.url](#)

[Information Security/Assurance Free Courses.pdf](#)

[Carnegie Mellon UniversityCERT Virtual Training Environment.url](#)

[Carnegie Mellon University/CERT FISMA Information Assurance Online Training Courses.url](#)

[Carnegie Mellon University/CERT Virtual Training Environment \(Computer Security Online Training Courses\)](#)

[Securing Cisco Routers Online Training.url](#)

[Securing Cisco LAN Switches Online Training.url](#)

[Computer Forensic Basic Tech Prep Online Training Course.url](#)

[Informit Security Reference Guide.url](#)

[SANS Information Security Reading Room.url](#)

[Petri Knowledgebase And IT Security Training.url](#)

**DOD 8570 INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM**

[DOD 8570.01 Information Assurance Workforce Improvement Program.url](#)

**DNI SPECIAL SECURITY CENTER TRAINING COURSES**

[DNI Security Training Courses.url](#) (Free For Government And Contractors)

**DEFENSE SECURITY SERVICE (DSS)**

[DSS Customizable Website Security Guide.url](#)

[DSS Customizable Website Security Guide Download.url](#)

[DSS Academy On-Line Security Training.url](#)

[DSS Marking Classified Information.url](#)

[DSS Basic Security Procedures Necessary For Keeping You Out of Trouble.pdf](#)

[DSS Protecting Secret And Confidential Documents Refresher Training.pdf](#)

[DSS Basic Information Security Training.pdf](#)

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA)**

[DISA IA Education, Training and Awareness.url](#)

[DISA Online Information Assurance Training.url](#)

[DISA Designated Approving Authority Training.url](#)

[DISA/DOD Free IA Training-Awareness Products Descriptions.pdf](#)

[DISA/DOD Free IA Training-Awareness Products Order Form.doc](#)

**ARMY**

[Army Information Assurance Security Officer \(IASO\) Training.url](#)

**NSA**

[NSA COMSEC Security Awareness Training.pdf](#)

[NSA COMSEC Awareness Exam.doc](#)

**IT SECURITY/INFORMATION SECURITY WEBSITES, MAGAZINES AND EBOOKS**

[IATAC Newsletters.url](#)

[Government Computer New/Security.url](#)

[Federal Computer Week/Security.url](#)

[WashingtonTechnology/Security.url](#)

[Information Security Magazine.url](#)

[SearchWindowsSecurity.url](#)

[WindowsITSecurity.url](#)

[WindowsSecurity.url](#)

[SecurityFocus.url](#)

[CSOnline.url](#)

[SCMagazine.url](#)

[Dark Reading.url](#)

[DEFCON Hacking Conference Media Archives.url](#)

[Black Hat Conference Multimedia Archives.url](#)

**EBOOKS**

[RealTimePublishers eBooks.url](#) (IT And Security Related Downloadable Books)

[RealTimePublishers eBooks.url](#) (Messaging/Web Security Downloadable Books And Podcasts)

## **FEDERAL GOVERNMENT AGENCIES**

## **INFORMATION SECURITY PROGRAM REFERENCES**

### **REFERENCE**

[Dept. Of Health Human Services Information Security-Privacy Program.url](#)

[Dept. Of Commerce Information Technology Security Program.url](#)

[Centers For Medicare & Medicaid Services Information Security.url](#)

[GSA Security Handbook And Standard Operating Procedures.pdf](#)

[Federal Agency Security Practices-1.url](#)

[Federal Agency Security Practices-2.url](#)

## **FEDERAL REGULATIONS AND GUIDANCE**

### **PUBLICS LAWS**

[Federal Information Security Management Act/FISMA.url](#)

[Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources.url](#)

[Applicable Laws And Guidance For US Government Information-Information Systems.pdf](#)

[IT Security Laws And Federal Regulations.pdf](#)

[NIST Laws, Regulations, And Directives.url](#)

[Public Laws - Library of Congress.url](#)

[Computer Fraud and Abuse Act.url](#)

[Code of Federal Regulations.url](#)

### **GENERAL SERVICES ADMINISTRATION (GSA)**

[GSA Reporting For Contractors.url](#)

[GSA Online Form For Government Contractors To Submit Evidence Of Possible Criminal Activities.url](#)

### **OFFICE OF MANAGEMENT AND BUDGET (OMB)**

[OMB Circulars.url](#)

[OMB Memoranda.url](#)

### **WHITE HOUSE**

[Presidential Executive Orders.url](#)

[National Security.url](#)

[Homeland Security.url](#)